Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

Governing for Enterprise Security

Julia H. Allen
Networked Systems Survivability
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Sponsored by the U.S. Department of Defense

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **JAN 2005**	2. REPORT TYPE	3. DATES COVERED **00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE **Governing for Enterprise Security (Briefing Charts)**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**29**	

Definition

“Directing and controlling an organization to establish and sustain a culture of security in the organization's conduct (beliefs, behaviors, capabilities, and actions)”

Builds upon and expands commonly described forms of governance including corporate governance, enterprise governance, and information technology (IT) governance

Questions to Ask

What is at risk?

How much security is enough?

How does an enterprise

- evolve its approach to security?
- achieve and sustain adequate security?

Questions to Ask

What is at risk?

How much security is enough?

How does an enterprise

- evolve its approach to security?
- achieve and sustain adequate security?

What Is At Risk?

- Trust
- Reputation; brand
- Shareholder/stakeholder value
- Market confidence, share, capitalization
- Regulatory compliance; fines, jail time
- Customer retention, growth
- Customer and partner identity, privacy
- Ability to offer, fulfill business transactions
- Staff morale

Trust

“The central truth is that information security is a means, not an end. Information security serves the end of trust. Trust is efficient, both in business and in life; and misplaced trust is ruinous, both in business and in life.

Trust makes it possible to proceed where proof is lacking. As an end, trust is worth the price. Without trust, information is largely useless.”

[Dan Geer; “Why Information Security Matters”]

Responsibility to Protect Digital Assets

Duty of Care: D&O Governance of Corporate Digital Security

- Govern business operations; protect critical assets
- Protect market share, stock price
- Govern employee conduct
- Protect reputation
- Ensure compliance requirements are met

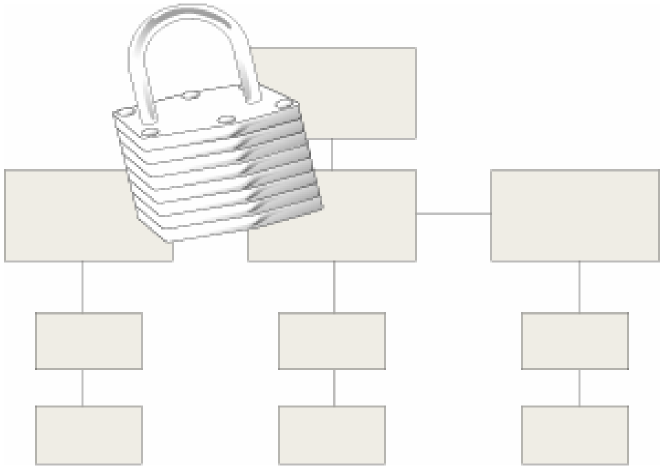
Business Judgment Rule: That which a reasonably prudent director of a similar corporation would have used

[Jody Westby, PricewaterhouseCoopers, Congressional Testimony; case law]

Barriers to Tackling Security

- Abstract, concerned with hypothetical events
- A holistic, enterprise-wide problem; not just technical
- No widely accepted measures/indicators
- Disaster-preventing rather than payoff-producing (like insurance)
- Installing security safeguards can have negative aspects (added cost, diminished performance, inconvenience)

Questions to Ask



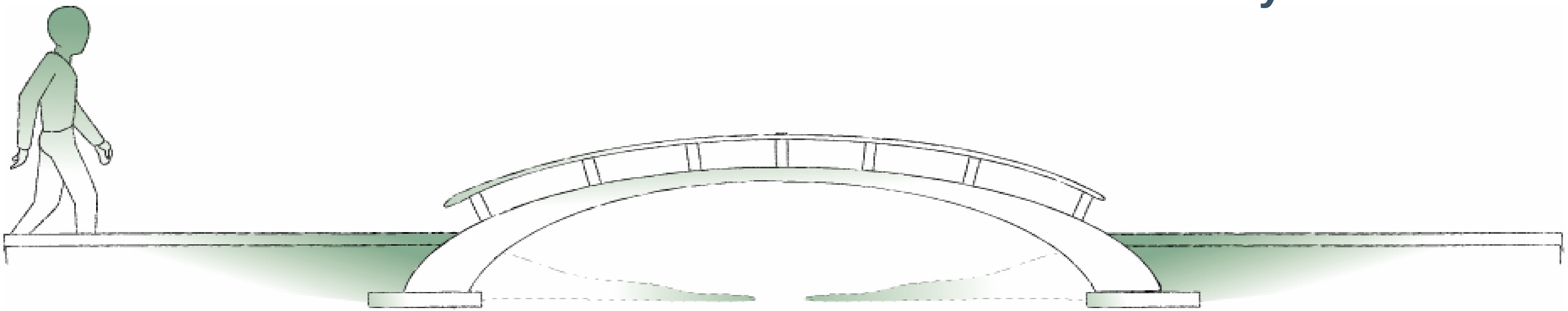
What is at risk?

How much security is enough?

How does an enterprise
- evolve its approach to security?
- achieve and sustain adequate security?

Shift the Security Perspective

	From →	*To*
Scope:	Technical problem	Enterprise problem
Ownership:	IT	Enterprise
Funding:	Expense	Investment
Focus:	Intermittent	Integrated
Driver:	External	Enterprise
Application:	Platform/practice	Process
Goal:	IT security	Enterprise continuity/resilience



Security *to* Resiliency

Managing to threat and vulnerability

No articulation of desired state

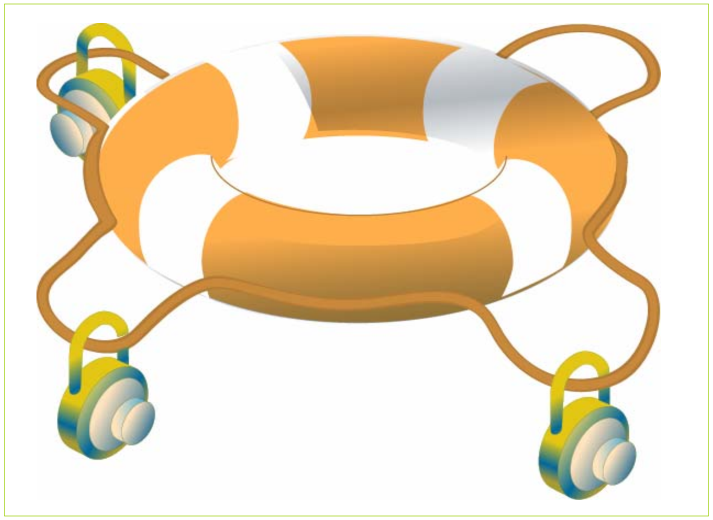
Possible security technology overkill

to →

Managing to impact and consequence

Adequate security defined as desired state

Security in sufficient balance to cost, risk



A Resilient Enterprise Is Able To. . .

- withstand systemic discontinuities and adapt to new risk environments [Starr 03]
- be sensing, agile, networked, prepared [Starr 03]
- dynamically reinvent business models and strategies as circumstances change [Hamel 04]
- have the capacity to change before the case for change becomes desperately obvious [Hamel 04]

Security Strategy Questions

- What needs to be protected? Why does it need to be protected? What happens if it is not protected?
- What potential adverse consequences need to be prevented? At what cost? How much disruption can we stand before we take action?
- How do we effectively manage the residual risk when protection and prevention actions are not taken?

Defining Adequate Security

The condition where the *protection strategies*

for an organization's critical *assets* and business *processes*

are commensurate with the organization's *risk appetite* and *risk tolerances*

Risk appetite and risk tolerance as defined by COSO’s Enterprise Risk Management Integrated Framework, September, 2004.

http://www.cert.org/governance/adequate.html

Determining Adequate Security Depends On . . .

- Enterprise factors: size, complexity, asset criticality, dependence on IT, impact of downtime

- Market sector factors: provider of critical infrastructure, openness of network, customer privacy, regulatory pressure, public disclosure

- Principle-based decisions: Accountability, Awareness, Compliance, Effectiveness, Ethics, Perspective/Scope, Risk Management, etc.

http://www.cert.org/governance/ges-aware.html

http://www.cert.org/governance/stakeholder.html

Adequate Security and Operational Risk

“Appropriate business security is that which protects the business from undue operational risks in a cost-effective manner.” [Sherwood 03]

“With the advent of regulatory agencies assessing a business’s aggregate operational risk, there needs to be a way of looking at the organization as a whole rather than its many parts.” [Milus 04]

[According to Basel II, operational risks are risks of loss resulting from inadequate or failed internal processes, people, and systems or from external events. http://www.bis.org/publ/bcbs107.htm]

Questions to Ask

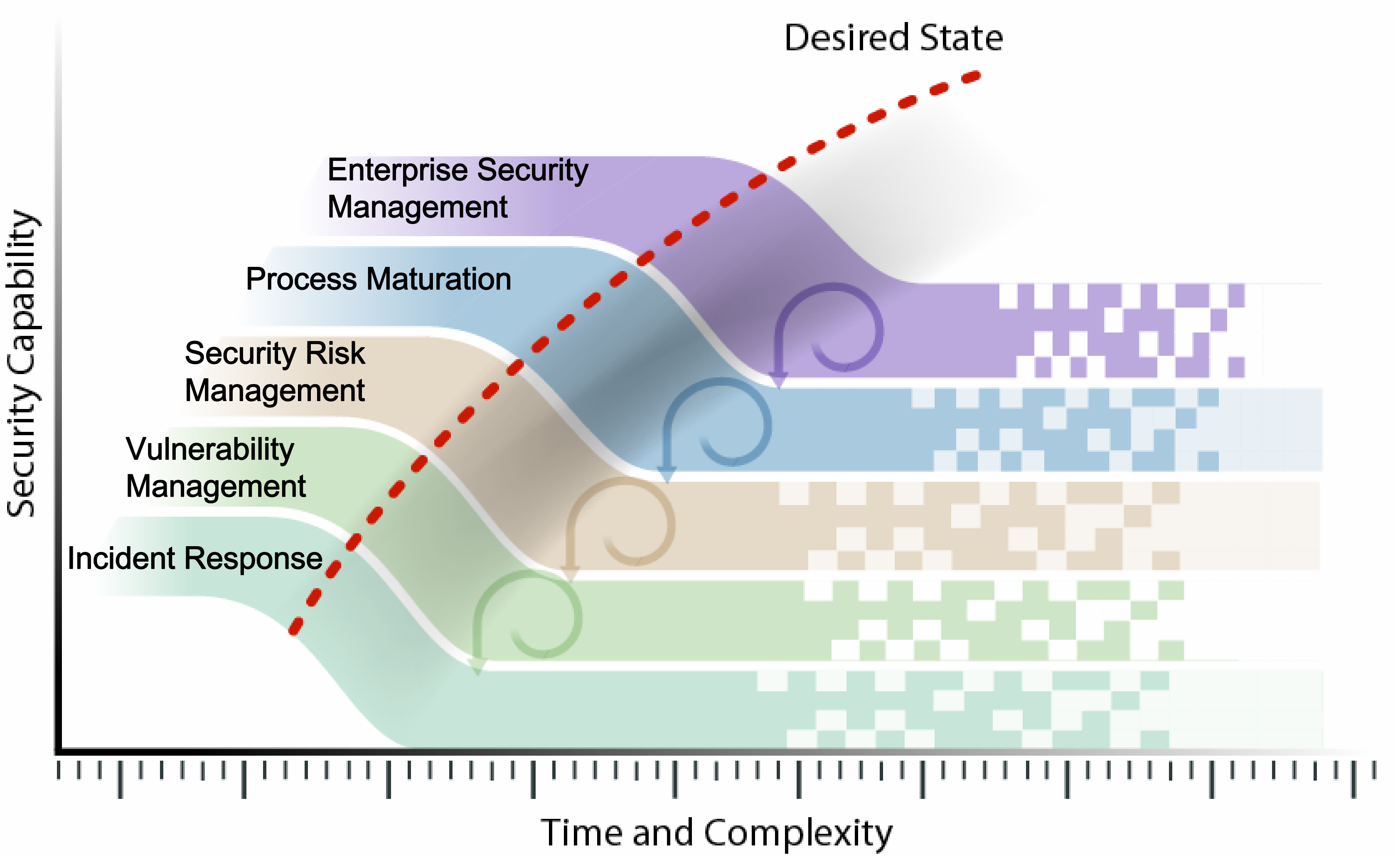
What is at risk?

How much security is enough?

How does an enterprise

- evolve its approach to security?
- achieve and sustain adequate security?

Evolving the Security Approach



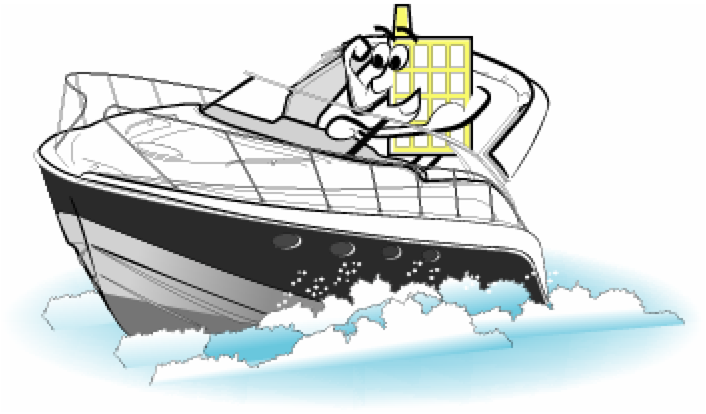
Questions to Ask

What is at risk?

How much security is enough?

How does an enterprise

- evolve its approach to security?
- achieve and sustain adequate security?

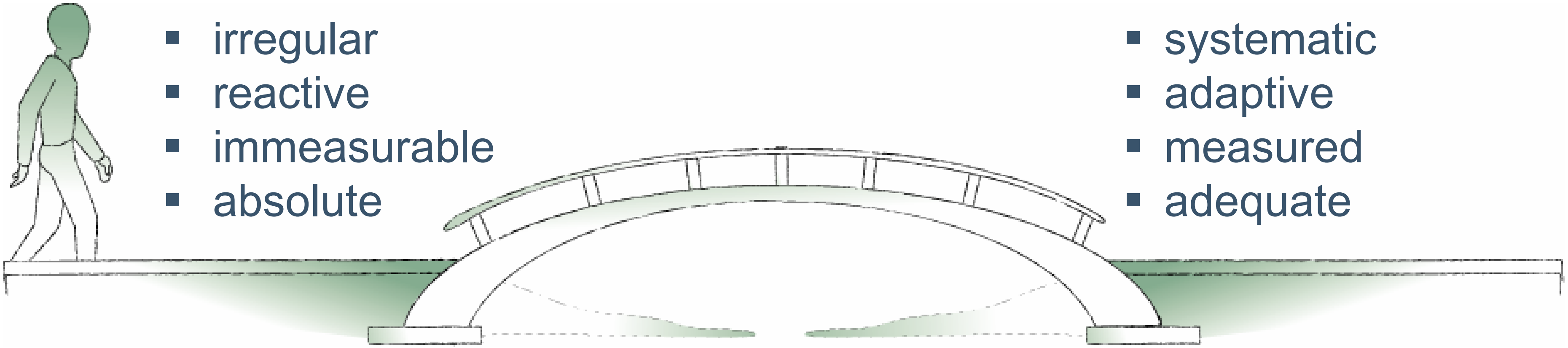


Shift the Security Approach

Ad-hoc and tactical

to →

Managed and strategic

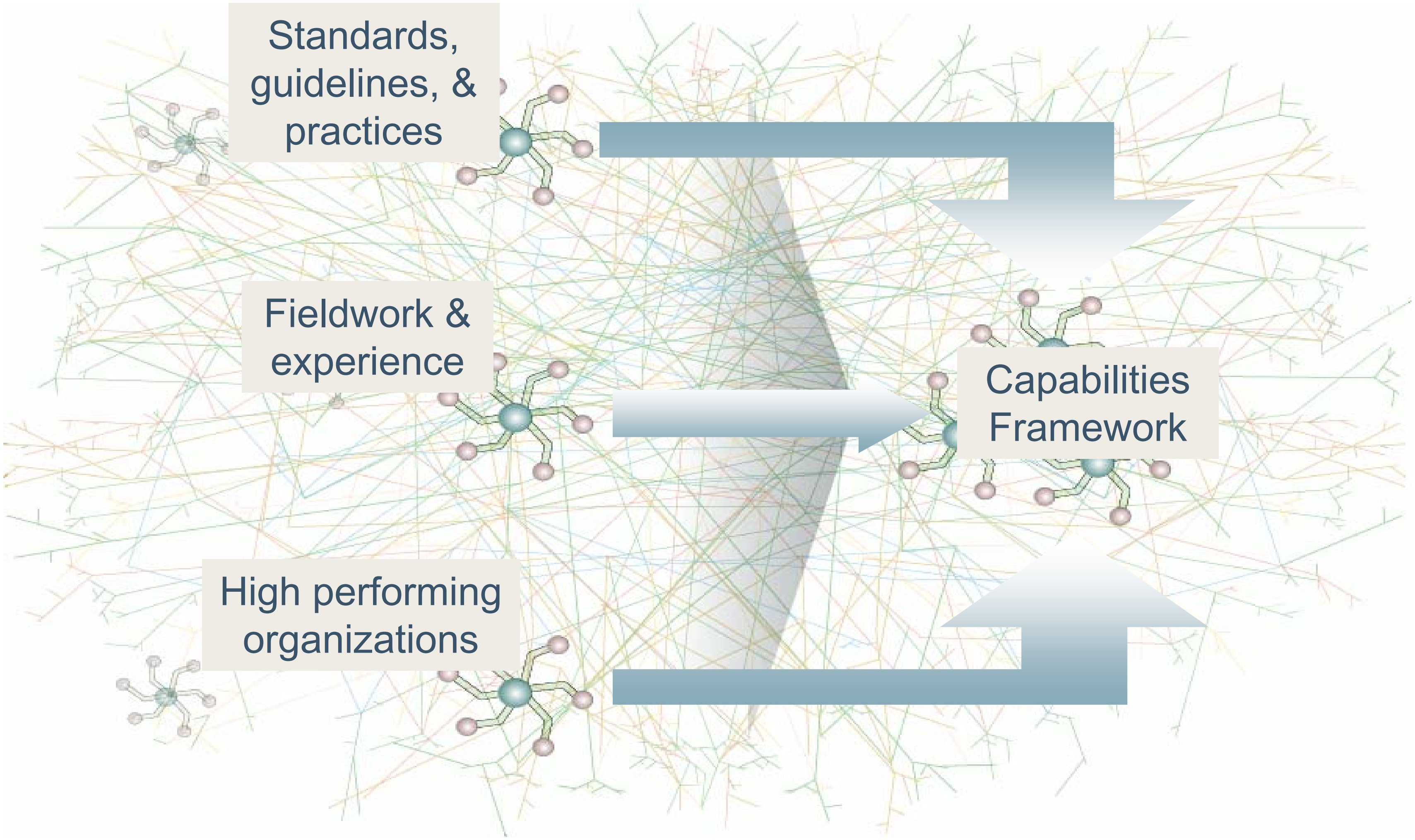


- irregular
- reactive
- immeasurable
- absolute

- systematic
- adaptive
- measured
- adequate

Security activities and measures of security performance are visibly aligned with strategic drivers and critical success factors.

Deriving a Framework


Standards, guidelines, & practices
Fieldwork & experience
High performing organizations
Capabilities Framework

Notional Set of Capabilities

Asset Management

Audit

Crisis Management

Enterprise Security Governance

IT Operations

Partner Management

Physical/Facilities Management

Process Management

Project Management

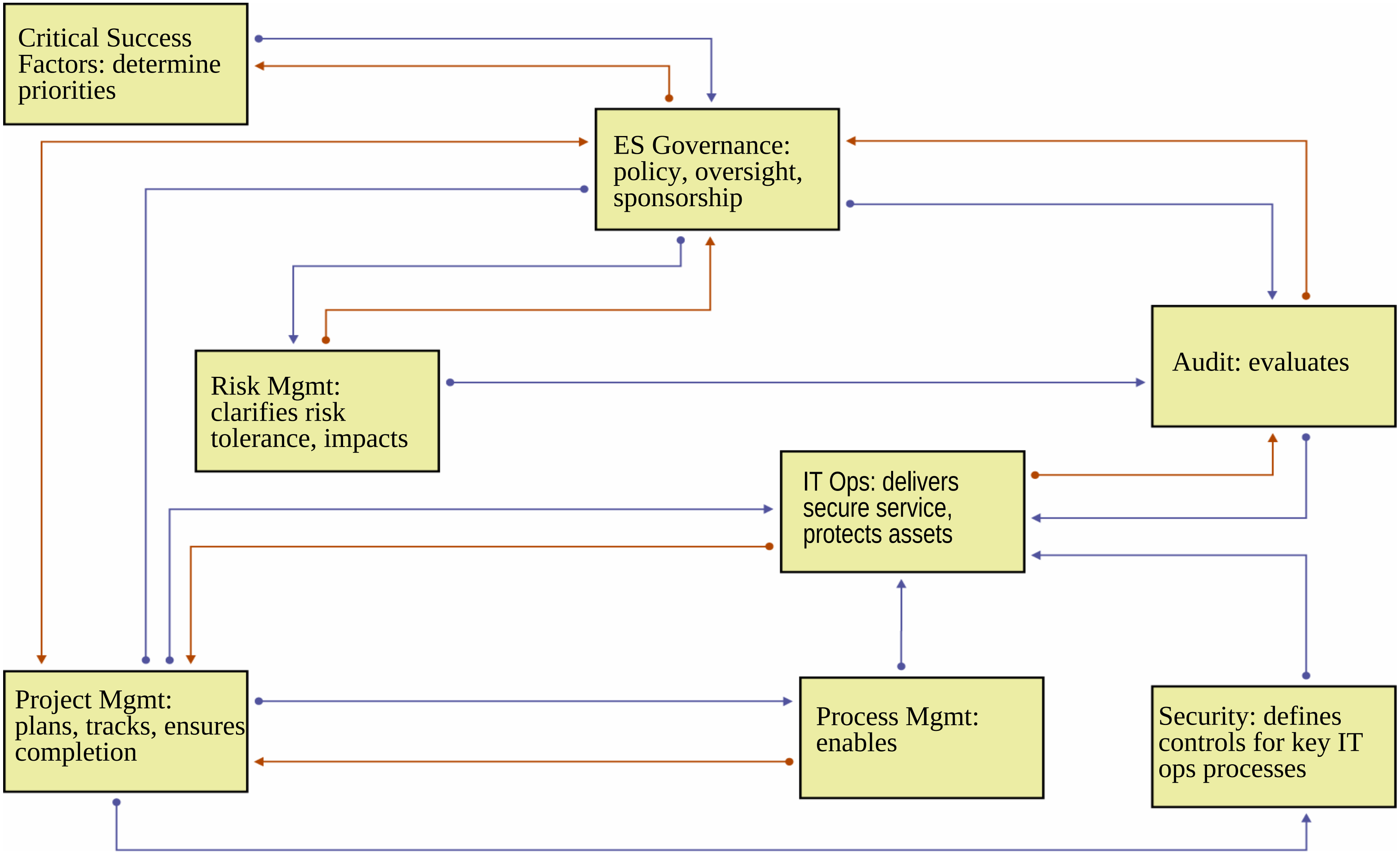
Risk Management

Security Operations

Systems Development

User Management

Mobilizing Capabilities to Achieve/Sustain Adequate Security



Critical Success Factors: determine priorities

ES Governance: policy, oversight, sponsorship

Risk Mgmt: clarifies risk tolerance, impacts

Audit: evaluates

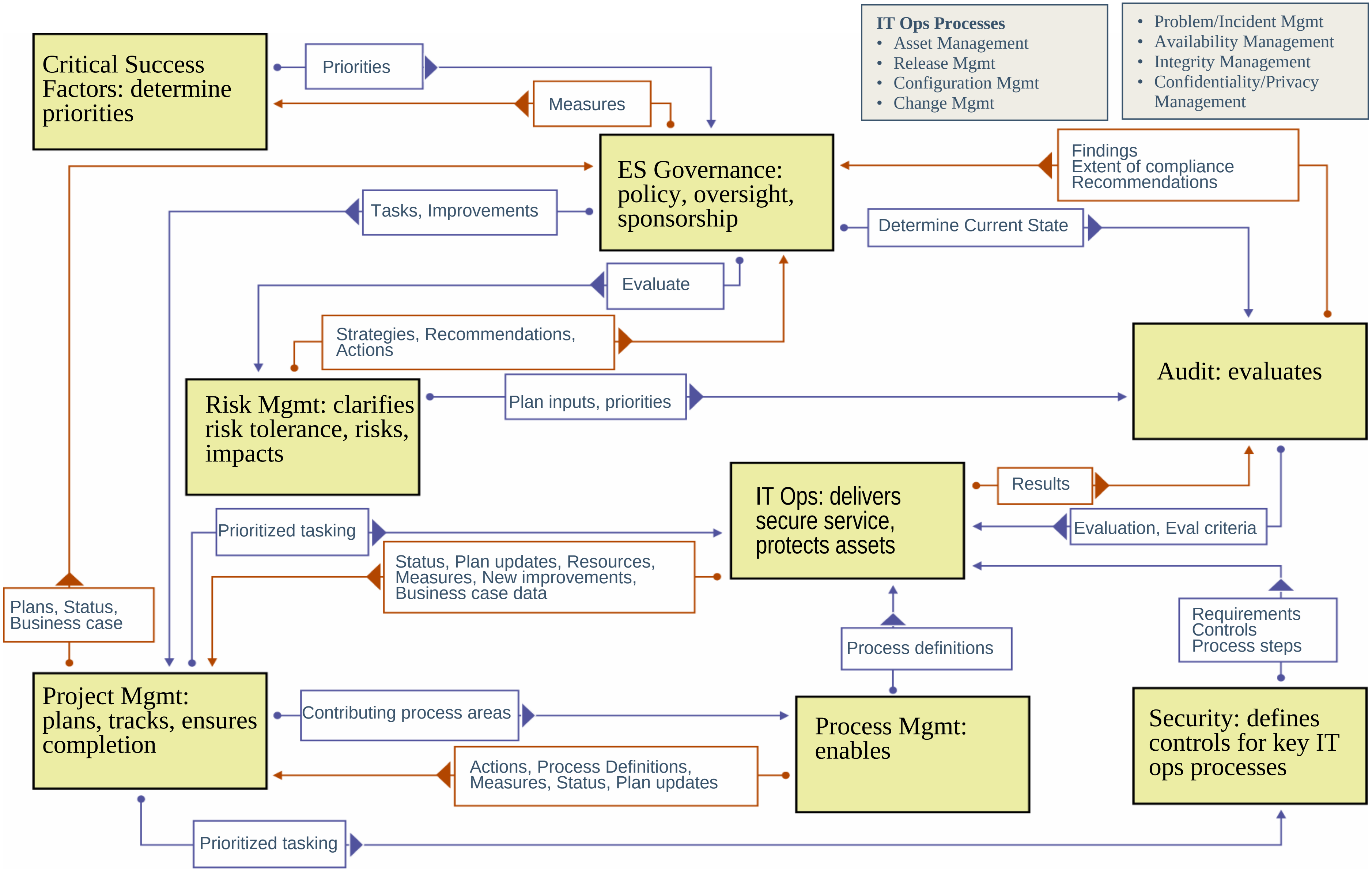
IT Ops: delivers secure service, protects assets

Project Mgmt: plans, tracks, ensures completion

Process Mgmt: enables

Security: defines controls for key IT ops processes

Mobilizing to Achieve/Sustain Adequate Security


IT Ops Processes
• Asset Management
• Release Mgmt
• Configuration Mgmt
• Change Mgmt
• Problem/Incident Mgmt
• Availability Management
• Integrity Management
• Confidentiality/Privacy Management
Critical Success Factors: determine priorities
Priorities
Measures
ES Governance: policy, oversight, sponsorship
Findings
Extent of compliance
Recommendations
Tasks, Improvements
Determine Current State
Evaluate
Strategies, Recommendations, Actions
Audit: evaluates
Risk Mgmt: clarifies risk tolerance, risks, impacts
Plan inputs, priorities
IT Ops: delivers secure service, protects assets
Results
Evaluation, Eval criteria
Prioritized tasking
Status, Plan updates, Resources, Measures, New improvements, Business case data
Plans, Status, Business case
Requirements
Controls
Process steps
Process definitions
Project Mgmt: plans, tracks, ensures completion
Contributing process areas
Process Mgmt: enables
Security: defines controls for key IT ops processes
Actions, Process Definitions, Measures, Status, Plan updates
Prioritized tasking

What Does Effective Security Look Like at the Enterprise Level?

- No longer solely under IT’s control
- Achievable, measurable objectives are defined and included in strategic and operational plans
- Functions across the organization view security as part of their job (e.g., Audit) and are so measured
- Adequate and sustained funding is a given
- Senior executives visibly sponsor and measure this work against defined performance parameters
- Considered a requirement of being in business

What Is Internal Audit's Role?

- Leverage Audit's professionalism and enterprise-wide scope
- Supplement compliance activities with risk assessment and process improvement
- Create an enterprise-wide risk-based audit program(*)
- Broaden audit scope to address third-party and vendor risk
- Collaborate with IT to mitigate information systems risk proactively

(*) including enterprise security

[PriceWaterhouseCoopers Internal Audit Global Best Practices; http://www.pwc.com/extweb/service.nsf/docid/D52A08081C25BC3885256F0B00522DF9]

Why Should Internal Audit Care?

Responsible for evaluating the adequacy and effectiveness of controls

- Reliability and integrity of financial, operational information
- Effectiveness, efficiency of operations
- Safeguarding assets
- Compliance with laws, regulations, contracts

Brings a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes

[IIA, Tone at the Top, Issue 23, October 2004.]

For More Information

- Governing for Enterprise Security (http://www.cert.org/governance/ges.html)
- Enterprise Security Management (http://www.cert.org/nav/index_green.html)
- CERT web site (http://www.cert.org); ITPI web site (http://www.itpi.org); SEI web site (http://www.sei.cmu.edu)
- jha@cert.org

The CERT® Guide to System and Network Security
Allen
E GUIDE FOR SENIOR MANAGERS
Top Ten Recommended Information Security Practices
1st Edition - July 2002
Years of Service 1988 - 2003

funded research and development center operated by Carnegie Mellon University.

What's New

January 13, 2004
System for Internet Level Knowledge (SiLK)
SiLK is a collection of netflow tools that facilitates security analysis in large networks.

November 24, 2003
CERT Summary CS-2003-04
Topics in this regularly scheduled CERT Summary include vulnerabilities in Microsoft Windows Workstation Service, RPCSS Service, and Exchange; a buffer overflow in Sendmail, and vulnerabilities in various SSL/TLS implementations.

October 17, 2003
Updated CERT/CC Statistics
Statistics have been added for the third quarter of 2003.

New & Home Users

Tech Tip:
Before You Connect a New Computer to the Internet

Article:
There IS an Intruder in My Computer – What Now?

CA-2004-01
Multiple H.323 Message Vulnerabilities

CA-2003-28
Buffer Overflow in Windows Workstation Service

CA-2003-27
Multiple Vulnerabilities in Microsoft Windows and Exchange

Vulnerability Notes

New and Notable Vulnerabilities:
Vulnerabilities in H.323 messaging
Microsoft IE URL display vulnerability
Integer overflow vulnerability in gsnlp
BIND DNS negative cache poisoning

all vulnerability notes

Current Activity
Tue Jan 20 17:48:47 EST 20
W32/Beagle or W32/Bagle Worm
Systems compromised via buffer overflow in DameWare

Current Activity Archive

Practices & Evaluations

octave risk evaluation method

References

[Hamel 04] Hamel, Gary; Valikangas, Liisa. “The Quest for Resilience,” Harvard Business Review, September 2003.

[Milus 04] Milus, Stu. “The Institutional Need for Comprehensive Auditing Strategies.” Information Systems Control Journal, Volume 6, 2004.

[Sherwood 03] Sherwood, John; Clark; Andrew; Lynas, David. “Systems and Business Security Architecture.” SABSA Limited, 17 September 2003. Available at http://www.alctraining.com.au/pdf/SABSA_White_Paper.pdf.

[Starr 03] Starr, Randy; Newfrock, Jim; Delurey, Michael. “Enterprise Resilience: Managing Risk in the Networked Economy.” strategy+business, Spring 2003. Also appears in “Enterprise Resilience: Risk and Security in the Networked World: A strategy+business Reader.” Randall Rothenberg, ed.

[Westby 04] Westby, Jody. “Information Security: Responsibilities of Boards of Directors and Senior Management.” Testimony before the House Committee on Government Reform: Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, September 22, 2004. Available at http://www.reform.house.gov/UploadedFiles/Westby1.pdf.